Splunk Enterprise Security Implementation Project

Project Overview

A comprehensive guide to implementing Splunk Enterprise for security monitoring with Security Onion integration, network monitoring, log analysis, and vulnerability management on a Kali Linux environment.

Table of Contents

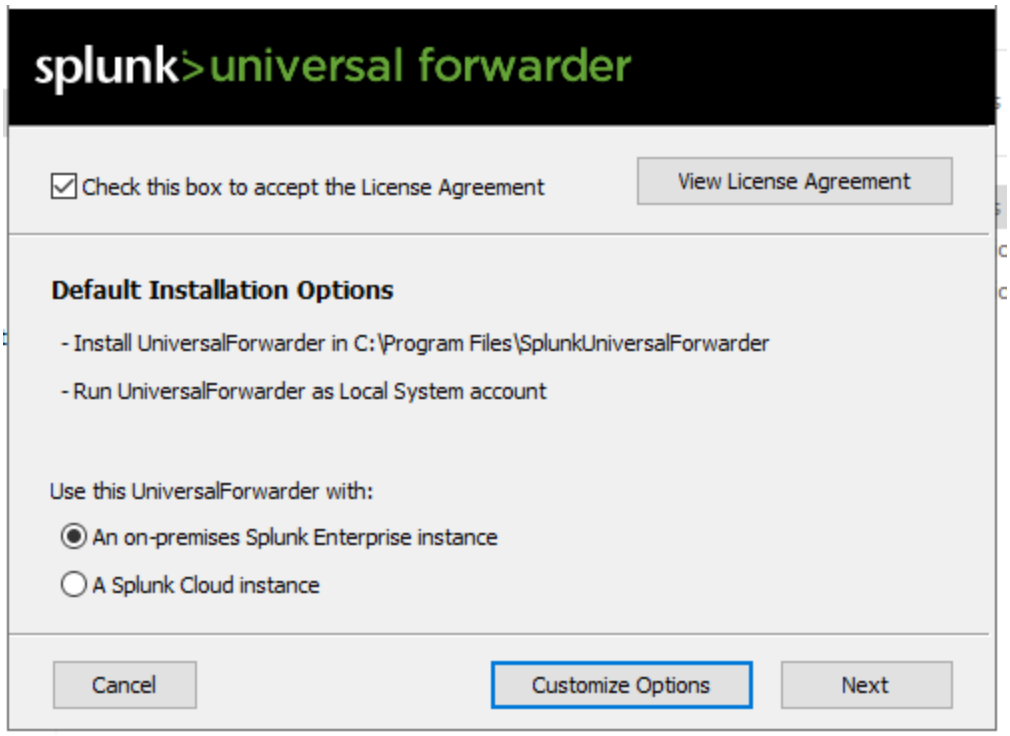
Initial Setup Steps

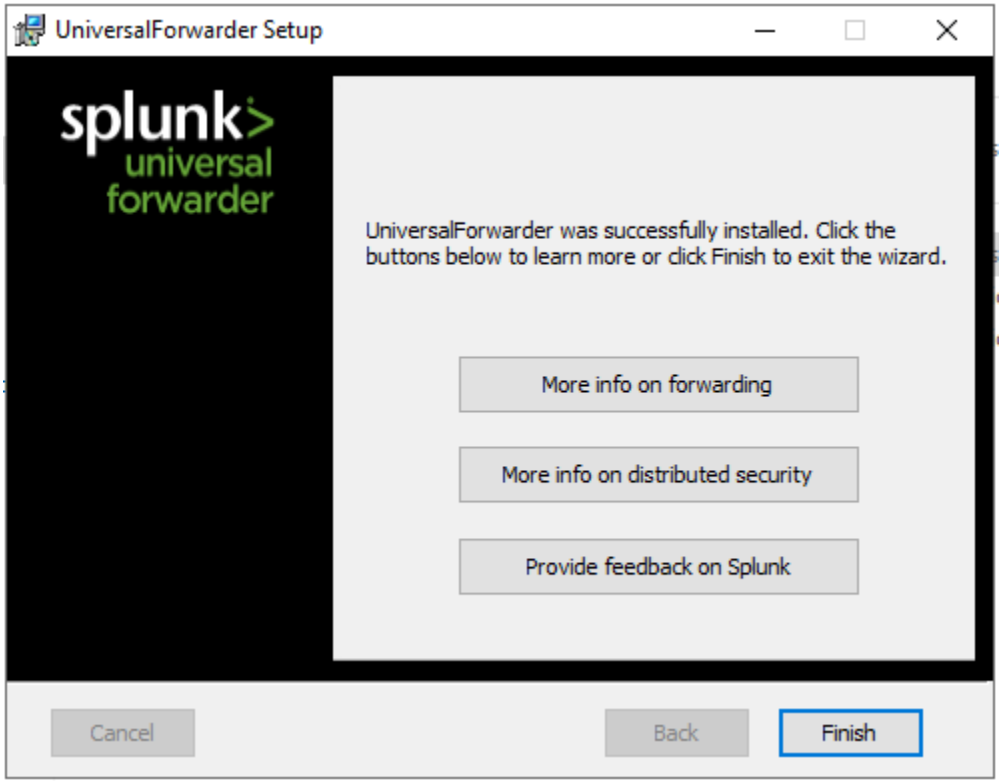
1. Download Splunk Enterprise on the Host PC

- Navigate to Splunk's official website
- Download the appropriate version for your operating system
- Verify system requirements (minimum 4GB RAM, 20GB disk space recommended)
- Save the installer to a designated directory

2. Download Splunk Universal Forwarder on Client PCs

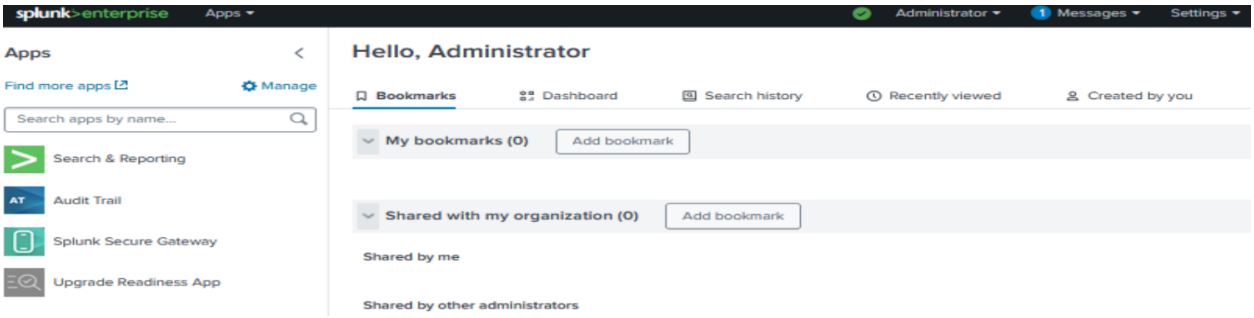
- Access Splunk downloads page
- Select Universal Forwarder for your client OS
- This lightweight agent will forward data to the Enterprise instance
- Document download locations for inventory purposes


splunk>universal forwarder
Check this box to accept the License Agreement
View License Agreement
Default Installation Options
- Install UniversalForwarder in C:\Program Files\SplunkUniversalForwarder
- Run UniversalForwarder as Local System account
Use this UniversalForwarder with:
An on-premises Splunk Enterprise instance
A Splunk Cloud instance
Cancel
Customize Options
Next


UniversalForwarder Setup
splunk> universal forwarder
UniversalForwarder was successfully installed. Click the buttons below to learn more or click Finish to exit the wizard.
More info on forwarding
More info on distributed security
Provide feedback on Splunk
Cancel
Back
Finish

3. Install Splunk on Host and Client PC

- **Host Installation**: Run the Enterprise installer with administrative privileges
- **Client Installation**: Deploy Universal Forwarder on each monitored endpoint
- Configure installation directories and service accounts
- Verify installations complete successfully



4. Create an inputs.conf File on the Client Device

bash

 # Example inputs.conf configuration

[monitor:///var/log]

disabled = false

index = main

sourcetype = syslog

[monitor:///var/log/apache2]

disabled = false

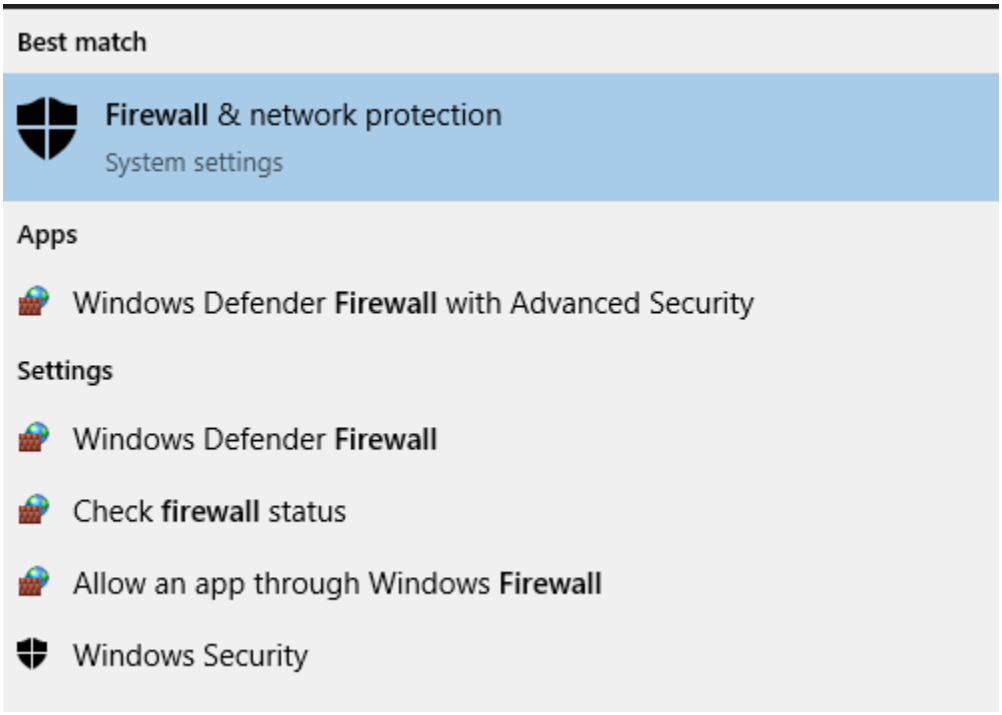
index = web_logs

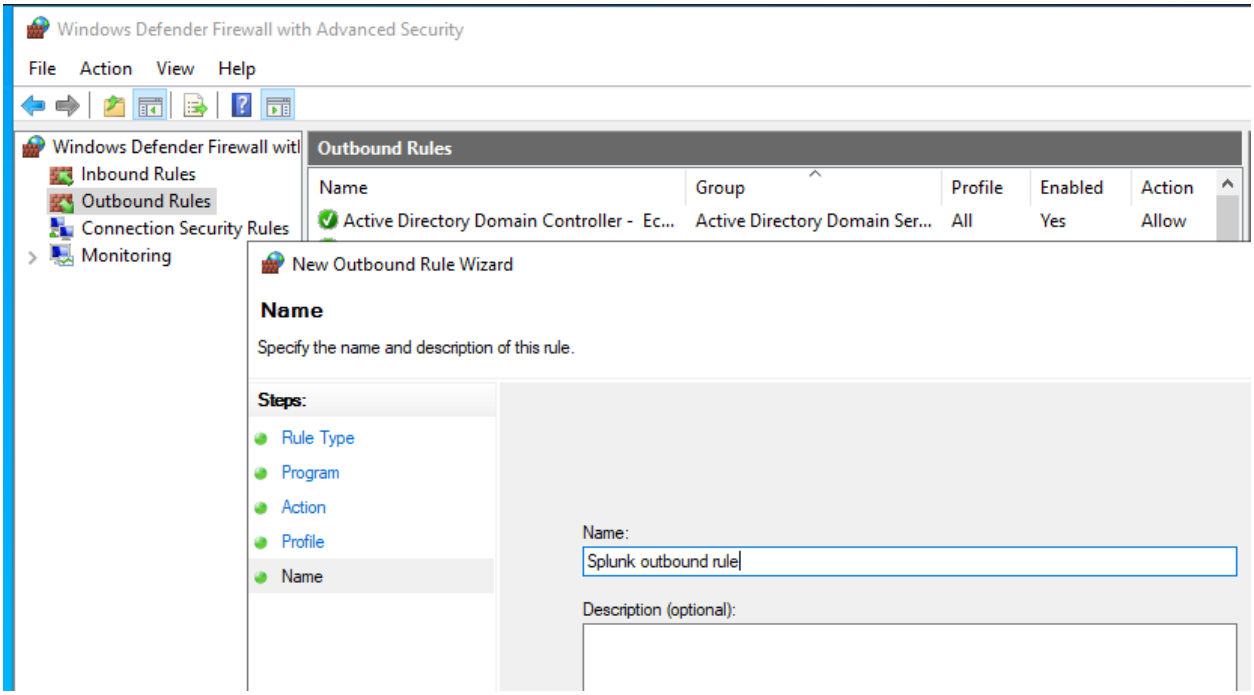
sourcetype = apache_access

5. Configure the Outbound Rule on the Client PC Firewall

- Allow outbound traffic on port 9997 (default Splunk forwarder port)
- Configure destination IP to point to Splunk Enterprise host
- Document firewall rule changes in your security policy

- Test connectivity after rule implementation



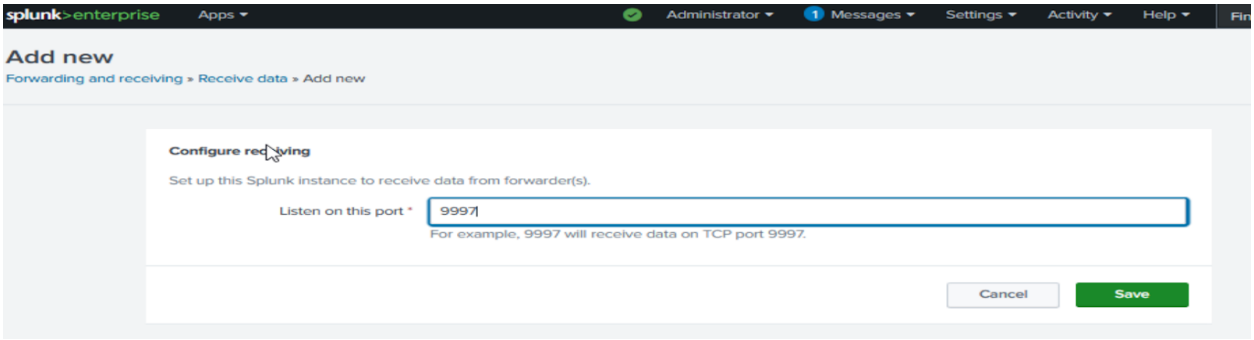


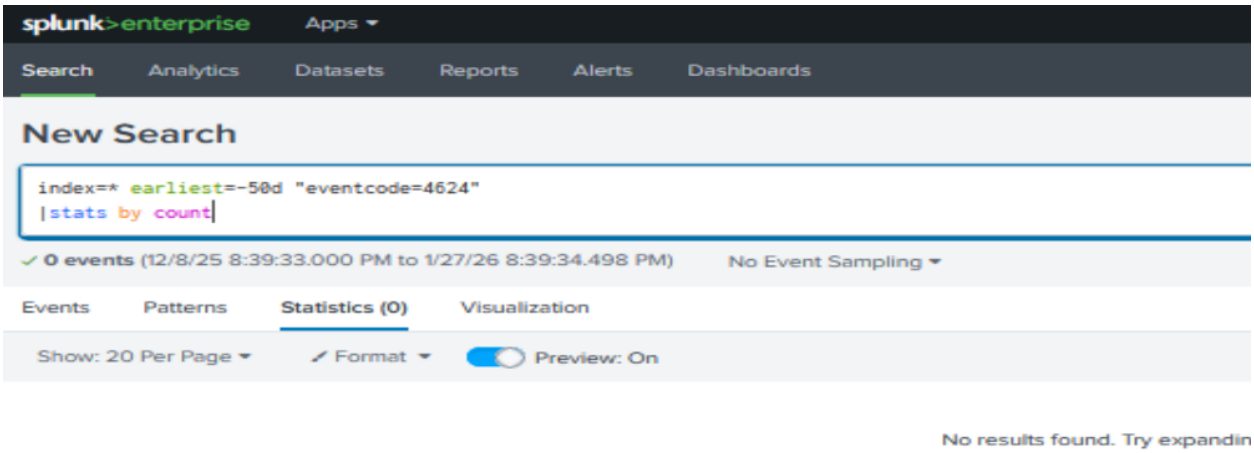
6. Setup the Indexer on the Host Splunk Application

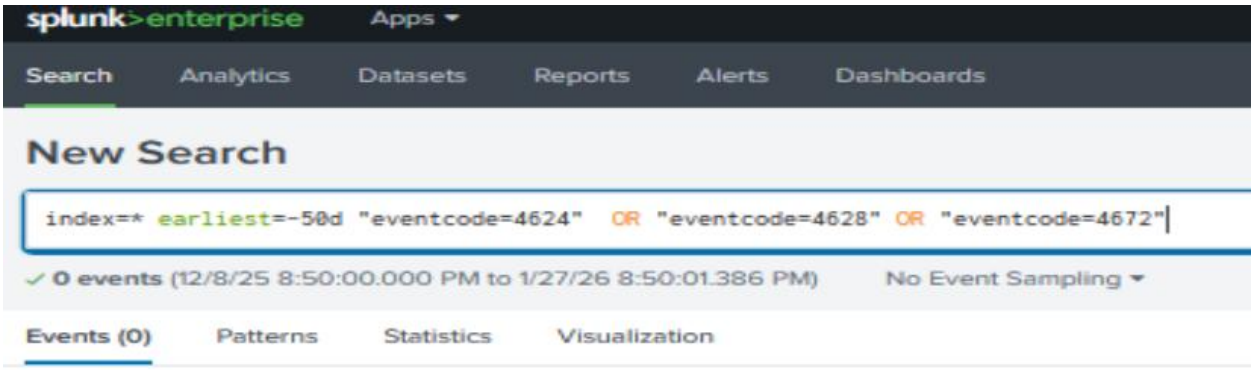
- Configure receiving on port 9997
- Create appropriate indexes for different data types
- Set retention policies based on compliance requirements
- Configure index sizing and storage allocation

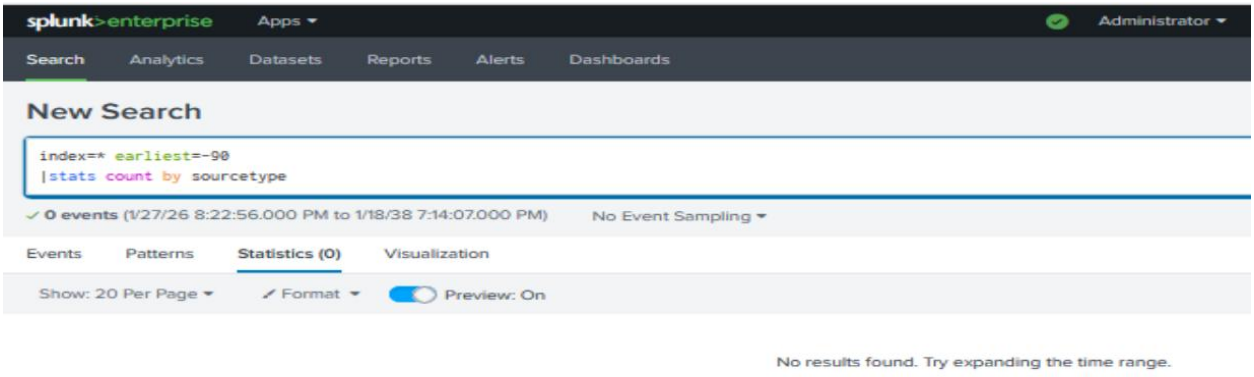
7. Configure Forwarding and Receiving Portal

- Enable receiving on Splunk Enterprise: Settings → Forwarding and Receiving → Configure Receiving
- Add port 9997 or your designated port
- On forwarders, configure deployment server for centralized management
- Test data flow from forwarders to indexers




splunk>enterprise
Apps
Search
Analytics
Datasets
Reports
Alerts
Dashboards
New Search
index=* earliest=-50d "eventcode=4624"
|stats by count
0 events (12/8/25 8:39:33.000 PM to 1/27/26 8:39:34.498 PM)
No Event Sampling
Events
Patterns
Statistics (0)
Visualization
Show: 20 Per Page
Format
Preview: On
No results found. Try expandin


splunk>enterprise
Apps
Search
Analytics
Datasets
Reports
Alerts
Dashboards
New Search
index=* earliest=-50d "eventcode=4624" OR "eventcode=4628" OR "eventcode=4672"
0 events (12/8/25 8:50:00.000 PM to 1/27/26 8:50:01.386 PM)
No Event Sampling
Events (0)
Patterns
Statistics
Visualization


splunk>enterprise
Apps
Administrator
Search
Analytics
Datasets
Reports
Alerts
Dashboards
New Search
index=* earliest=-90
|stats count by sourcetype
0 events (1/27/26 8:22:56.000 PM to 1/18/38 7:14:07.000 PM)
No Event Sampling
Events
Patterns
Statistics (0)
Visualization
Show: 20 Per Page
Format
Preview: On
No results found. Try expanding the time range.

8. Configure the Inbound Rule of the Firewall of the Client

- Allow inbound management traffic if using deployment server
- Configure port 8089 for Splunk management (if needed)
- Restrict access to authorized Splunk infrastructure IPs only
- Document all firewall modifications

Architecture Overview

Environment Details

- **Platform**: Kali Linux Oracle Virtual Machine
- **Primary Components**:
    - Splunk Enterprise (Host/Indexer)
    - Splunk Universal Forwarder (Clients)
    - Security Onion (Network Security Monitoring)
    - Splunk Dashboard & Filters

Integration Points

- Security Onion feeds network traffic analysis data
- Universal Forwarders send endpoint logs
- Centralized indexing and correlation on Enterprise instance
- Real-time alerts and dashboards for security events

Implementation Process

Phase 1: Planning & Preparation

Definition of Scope:

- Identify all systems requiring monitoring
- Define log sources (system logs, application logs, network traffic, security events)

- Establish data retention requirements based on compliance needs (ISO 27001, NIST CSF, etc.)
- Create network diagrams showing data flows

Resource Allocation:

- Determine hardware/VM requirements for indexers and search heads
- Calculate storage needs based on daily log ingestion rates
- Plan for redundancy and disaster recovery

Phase 2: Installation & Configuration

Step-by-Step Process:

1. **Prepare the Virtual Environment**
    - Set up Kali Linux Oracle VM with adequate resources
    - Configure network interfaces for monitoring and management
    - Install required dependencies and updates
2. **Deploy Splunk Enterprise**
    - Install on host system
    - Configure initial admin credentials
    - Set up licensing (enterprise trial or production license)
3. **Deploy Universal Forwarders**
    - Install on all client endpoints
    - Configure inputs.conf for relevant log sources
    - Set up outputs.conf to point to indexer
4. **Configure Data Inputs**
    - System logs: /var/log/syslog, /var/log/auth.log
    - Application logs: Apache, Nginx, custom applications
    - Network data: Integrate Security Onion IDS/IPS alerts
    - Security events: Failed login attempts, privilege escalations

Phase 3: Security Onion Integration

Network Monitoring Setup:

- Deploy Security Onion on a separate VM or host
- Configure network taps or SPAN ports for traffic capture
- Set up Snort/Suricata IDS rules
- Forward Security Onion alerts to Splunk via syslog or HTTP Event Collector

Data Sources to Monitor:

- Network traffic metadata
- IDS/IPS alerts
- Full packet capture (for forensic analysis)
- DNS queries and HTTP transactions

Security Best Practices

During Scanning Operations

Pre-Scan Preparation:

- Document baseline network behavior
- Notify stakeholders of scanning activities
- Ensure proper authorization for vulnerability scanning
- Configure scan policies to avoid service disruption

Important Information to Monitor:

- Authentication attempts (successful and failed)
- Privilege escalation events
- Network connection patterns
- File integrity changes
- Process executions and anomalies

Post-Scan Analysis:

- Review scan results in Splunk dashboards
- Correlate vulnerability findings with actual exploitation attempts
- Prioritize remediation based on risk scoring
- Document findings in a structured format

How to Use Collected Information

1. **Threat Detection**: Create correlation searches for attack patterns
2. **Incident Response**: Use historical data to trace attack timelines
3. **Compliance Reporting**: Generate audit reports for regulatory requirements
4. **Capacity Planning**: Analyze trends to predict resource needs
5. **Security Posture Assessment**: Identify gaps in monitoring coverage